

What is claimed is:

- 5
1. A method, comprising:
- determining a set of arguments for an outsourced computation;
- preparing a group of disguised arguments corresponding to the set of arguments with a first computer;
- outputting the disguised arguments from the first computer for performance of the outsourced computation; and
- receiving a result of the outsourced computation performed with the disguised arguments.
- 10
2. The method of claim 1, further comprising computing an actual answer from the result after said receiving.
- 15
3. The method of claim 1, wherein said preparing includes:
- classifying the outsourced computation into one of a number of computation types;
- selecting one or more of a number of disguising operations based on said classifying; and
- 20 performing the one or more disguising operations on the actual arguments with the first computer to provide the disguised arguments.
4. The method of claim 3, wherein the computation types include matrix multiplication, matrix inversion, and convolution.

5. The method of claim 4, wherein the computation types further include solution of a system of linear equations, solution of one or more differential equations, quadrature, image edge detection, character string pattern matching, and sorting.

6. The method of claim 1, further comprising:
receiving the disguised arguments at a second computer remotely located relative to the first computer;

performing the outsourced computation with the second computer; and
sending the result from the second computer to the first computer, the result being in a disguised form relative to an answer obtained by submitting the actual arguments to the outsourced computation.

7. The method of claim 1, wherein said preparing includes generating a plurality of random numbers, the random numbers each being generated by one of a number of random number generation techniques, the techniques each including a different distribution parameter.

8. The method of claim 7, wherein said preparing further includes defining a number of disguise functions with one or more of the random numbers.

9. The method of claim 1, wherein said preparing includes modifying a linear operator.

10. The method of claim 1, wherein said preparing includes altering a dimension corresponding to the actual arguments to provide the disguised arguments.

11. The method of claim 10, wherein said altering includes expanding the dimension.

12. The method of claim 1, wherein said preparing includes performing a function substitution in accordance with at least one mathematical identity.

13. A method, comprising:

operating a first computer in accordance with one or more instructions to perform an outsourced mathematical computation, the first computer receiving a number of disguised arguments that hide a group of actual arguments for the outsourced mathematical computation;

performing the outsourced mathematical operation on the disguised arguments with the first computer; and

outputting a result of the outsourced mathematical computation with the first computer.

14. The method of claim 13, further comprising:

preparing the disguised arguments from the actual arguments with a second computer;

sending the disguised arguments to the first computer from the second computer;

receiving the result at the second computer; and
computing an actual answer from the result with the second computer.

15. The method of claim 13, wherein the outsourced mathematical computation
5 corresponds to at least one of the group consisting of matrix multiplication, matrix
inversion, and convolution.

16. The method of claim 13, wherein the outsourced mathematical computation
10 corresponds to at least one of the group consisting of solution of a differential
equation, quadrature, character string pattern matching, and image edge detection.

17. The method of claim 13, wherein the outsourced mathematical computation
corresponds to at least one of the group consisting of solution to a system of linear
equations and sorting.

18. A system, comprising:

a computer operable to define a set of actual arguments for an outsourced
computation, said computer being programmed to determine a group of disguised
arguments from the set of actual arguments, said disguised arguments hiding one or
20 more characteristics of the set of actual arguments;

an output device responsive to said computer to output the disguised
arguments for remote performance of said outsourced computation;

an input device to receive a result of said outsourced computation performed
with said disguised arguments; and

wherein said computer is responsive to said input device to determine a desired answer from said result.

a²
19. The system of claim 18, wherein said computer is further programmed to
5 classify said outsourced computation as being one of a number of types, said types including at least one of matrix multiplication, matrix inversion, and convolution.

20. The system of claim 18, further comprising a computing center, said
10 computing center being programmed to perform said outsourced computation with said disguised arguments.

21. The system of claim 18, wherein said computer includes a memory, a library
15 of disguise operations being stored in said memory, said computer programming referencing said library to generate said disguised arguments.

22. The system of claim 21, wherein said disguise operations correspond to at
least one of the group consisting of random object generation, argument dimension
modification, mathematical identity substitution, and disguise function generation.

20 23. The system of claim 18, wherein said computer includes instructions to generate a cubic spline to provide a disguise for said actual arguments.

24. A system, comprising:
an input device to receive a plurality of disguised arguments, said disguised

arguments hiding at least one characteristic of each of a number of actual arguments;
a computer responsive to programming to perform an outsourced computation
with said disguised arguments and provide a result of said outsourced computation;
and
5 an output device responsive to said computer to output said result for
conversion to a desired answer corresponding to said actual arguments..

25. The system of claim 24, further comprising another computer programmed to
generate said disguised arguments from said actual arguments.

10 26. The system of claim 24, wherein said computer is operable to perform a
number of different types of said outsourced computation, said types including matrix
multiplication, matrix inversion, and convolution.

15 27. The system of claim 24, wherein said programming includes a number of
routines each corresponding to a different type of said outsourced computation, said
routines corresponding to at least one of the group consisting of quadrature, solution
of a differential equation, solution of a system of linear equations, image edge
detection, character string pattern matching, and sorting.

20 28. An apparatus, comprising: a computer readable medium, said medium
defining computer programming instructions to hide a group of actual arguments for a
computation to be outsourced, said instructions being operable to generate a group of
disguised arguments corresponding to said actual arguments, said disguised

arguments being generated to provide a disguised result when provided for said computation, an actual answer being recoverable from said disguised result in accordance with said instructions, said actual answer being returned by said computation when said computation is provided said actual arguments.

5

29. The apparatus of claim 28, further including a computer responsive to said programming instructions.

30. The apparatus of claim 28, wherein said programming instructions are executable to classify said computation into at least one of a plurality of computation types, said computation types including matrix multiplication, matrix inversion, and convolution.

31. The apparatus of claim 28, wherein said programming instructions further define a library of disguise operations, said disguise operations corresponding to at least one of the group consisting of random object generation, dimension modification, and mathematical identity substitution.

32. The apparatus of claim 28, wherein said programming instructions define a routine to generate a cubic spline to provide at least one disguise function.

33. The apparatus of claim 28, wherein said programming instructions define a routine to provide a random function space to provide one or more disguise functions.